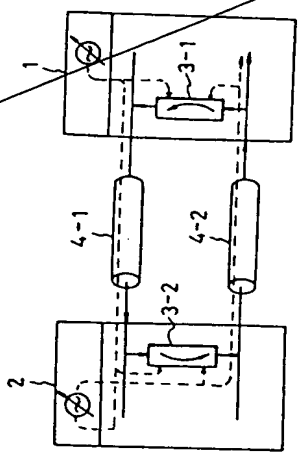
(54) **LOOP BACK CONTROL SYSTEM**
(11) **2-82834 (A)** (43) 23.3.1990 (19) JP
(21) Appl. No. 63-233684 (22) 20.9.1988
(71) NEC CORP (72) NORITOSHI DOUMORI
(51) **Int. Cl⁵. H04L7/00**

PURPOSE: To enable communication by loop back control independently of distinct of master station or slave station by incorporating a buffer memory circuit in a loop back circuit and holding the subordinate synchronization of an internetwork clock.

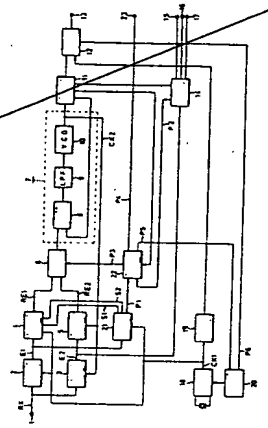
CONSTITUTION: The communication between a master station equipment 1 and a slave station equipment 2 is implemented normally through transmission lines 4-1, 4-2 and loop back circuits 3-1, 3-2 reflect respectively a reception signal to an opposite equipment at the time of loop back instruction. When the slave station equipment 2 receives a loop back instruction and the loop back circuit 3-2 is active, the loop back circuit 3-2 writes the reception signal in a buffer memory according to a subordinate clock from the master station equipment 1, read out by an output clock of the slave station equipment 2 and sent to an opposite equipment as a transmission signal. Moreover, the operation of the loop back circuit 3-1 of the master station equipment 1 is similar to above, the reception signal from the slave station equipment 2 is written in the buffer memory of the loop back circuit 3-1, read out by a transmission clock of the master station equipment 1 and folded to the slave station equipment 2.



(54) **DIGITAL SIGNAL RECEIVER**
(11) **2-82835 (A)** (43) 23.3.1990 (19) JP
(21) Appl. No. 63-235425 (22) 20.9.1988
(71) SONY CORP (72) TADATAKA FUJIYAMA
(51) **Int. Cl⁵. H04L7/033//G11B20/10**

PURPOSE: To supply a reference signal corresponding to an input digital signal to a PLL by using a table clock signal and discriminating a sampling frequency from a preamble of the input digital signal to form the reference signal.

CONSTITUTION: The length of a maximum inversion interval is measured by a stable clock signal CK1 generated from a clock generating circuit 18, a sampling frequency Fs is discriminated to form detection signals S1 and S2. A window generating circuit 4 generates a signal at (Fs=48kHz or 44.1kHz) and a signal at (Fs=32kHz) from a stable clock CK1, one of the signals is selected by the detection signals S1 and S2 and becomes a reference signal RE1. A window generating circuit 5 generates a reference signal RE2 from an output signal CK2 of a PLL 7. Thus, no accuracy is deteriorated alike the time constant of a monostable multivibrator. Moreover, since no monostable multivibrator is employed, the receiver is suitable for circuit integration.

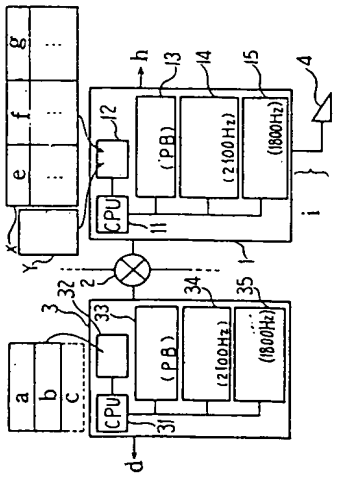


2,3: edge detection, 21: Tmax detection, 6: selector, 22: unlock detection, 8: phase comparator, 11: timing generator, 12: selector, 14: demodulator, 19: timing generator, 20: clock control

(54) **SECURITY GUARD SYSTEM FOR NETWORK**
(11) **2-82836 (A)** (43) 23.3.1990 (19) JP
(21) Appl. No. 63-235354 (22) 20.9.1988
(71) FUJITSU LTD (72) HIDEO OKI(2)
(51) **Int. Cl⁵. H04L9/06,H04L9/14,H04M3/42**

PURPOSE: To minimize the damage due to interception by sending security information for revising a cryptographic pattern to an exchange or a node and a network connection adaptor from a console of the exchange or the node to revise the cryptographic pattern.

CONSTITUTION: A maintenance console 4 generates the security information to be set or revised and a call to a network connection adaptor 3 corresponding to a terminal equipment of the user number is given by automatic dialing. A CPU 11 of a PBX 1 receives a cryptographic pattern number sent automatically from the console 4, a table Y constituting a security table is retrieved, a cryptographic pattern is extracted, a user code corresponding to the user number stored in a terminal management table X is converted and the result is sent to the adaptor 3. Then an old cryptographic pattern number corresponding to the user number is replaced into a cryptographic pattern number set newly.



a: cryptographic user code, b,g: cryptographic pattern number, c: system identifier, 32,12: memory, 33: revision information telegraphic section, 34: normal incoming identification signal reception section, 35: cryptographic revision notice reception section, 13: revision information generating section, 14: normal incoming identification signal generating section, 15: cryptographic revision notice generating section, e: user number, f: user code, h: terminal equipment, i: user number, cryptographic pattern number, system identifier

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−82836

⑤Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)3月23日
H 04 L 9/06 9/14			
H 04 M 3/42	E	7925−5K	
		7240−5K　H 04 L 9/02	Z

審査請求　未請求　請求項の数 2　(全7頁)

⑭発明の名称　ネットワークのセキュリテイ・ガード方式

⑳特　願　昭63−235354
㉒出　願　昭63(1988)9月20日

㉒発明者　大木　秀夫　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉒発明者　桑原　茂樹　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉒発明者　植村　篤　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉑出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
㉔代理人　弁理士　茂泉　修司

明　細　書

1．発明の名称

ネットワークのセキュリティ・ガード方式

2．特許請求の範囲

(1)端末(TE)に接続された網制御装置(NCU)の網接続アダプタ(3)から自営ネットワーク又は閉域ネットワーク(NW)の交換機又はノード(1)に公衆網(2)上のアクセスポイントを介してアクセスする時に暗号化されたセキュリティ情報を送出し該交換機又はノード(1)で復号してセキュリティテーブルと照合するネットワークのセキュリティ・ガード方式において、

該交換機又はノード(1)の側に設置された保守コンソール(4)から該交換機又はノード(1)に所定のアダプタ(3)の変更すべきセキュリティ情報を入力して対応する該セキュリティテーブルを変更するとともに該セキュリティテーブルに基づいて対応する該アダプタ(3)の　号化されたセキュリティ情報の設定・変更を行うことを特徴としたネットワークのセキュリティ・ガード方式。

(2)該ネットワーク(NW)に固有の識別子を該網接続アダプタ(3)に予め設定しておき、該変更の前に該コンソール(4)から該交換機又はノード(1)を介して該アダプタ(3)に該識別子を送り、該アダプタ(3)において該識別子の照合を行い一致した時のみ該設定・変更を行うことを特徴とした請求項1記載のネットワークのセキュリティ・ガード方式。

3．発明の詳細な説明

〔概　要〕

端末に接続された網制御装置の網接続アダプタから自営ネットワーク又は閉域ネットワークの交換機又はノードに公衆網上のアクセスポイントを介してアクセスする時に暗号化されたセキュリティ情報を送出し該交換機又はノードで復号してセキュリティテーブルと照合するネットワークのセキュリティ・ガード方式に関し、

暗号化されたセキュリティ情報が盗用される被

害を最小限にすることを目的とし、

該交換機又はノードの側に設置された保守コンソールから該交換機又はノードに所定のアダプタの変更すべきセキュリティ情報を入力して対応する該セキュリティテーブルを変更するとともに該セキュリティテーブルに基づいて対応する該アダプタの暗号化されたセキュリティ情報の設定・変更を行うように構成する。

〔産業上の利用分野〕

本発明はネットワークのセキュリティ・ガード方式に関し、特に端末に接続された網制御装置の網接続アダプタから自営ネットワーク又は閉域ネットワークの交換機又はノードに公衆網上のアクセスポイントを介してアクセスする時に暗号化されたセキュリティ情報を送出し該交換機又はノードで復号してセキュリティテーブルと照合するネットワークのセキュリティ・ガード方式に関するものである。

近年、公衆網を利用して自営ネットワーク又は閉域ネットワークを構築するシステムが増加しており、これに伴って斯かるシステムでの通信／通話情報の盗用を防止するため、利用者コード等のセキュリティ情報を用いてガードしているが、これらの利用者コードも盗用されることがあり、より一層のセキュリティを向上させる必要がある。

〔従来の技術〕

第７図には公衆網を利用して構築された自営ネットワーク又は閉域ネットワークＮＷが示されており、公衆網２の端末ＴＥ／ＴＥＬの側に収容した網制御装置ＮＣＵ中に網接続アダプタ３を設け、このアダプタ３及びネットワークＮＷのアクセスポイントＡＰに位置する交換機又はネットワークノード１により端末ＴＥ／ＴＥＬとネットワークＮＷ中の端末ＴＥ／ＴＥＬ又はホストコンピュータＨＣとの通信接続を行っている。

このようなネットワークシステムにおける従来のセキュリティ・ガード方式の接続動作を第８図の概念図及び第９図のシーケンス図により説明すると、端末ＴＥ／ＴＥＬ（左側）から希望の端末ＴＥ／ＴＥＬ（右側）の相手先番号をアダプタ３に対して発呼すると、アダプタ３では対応する自営／閉域ネットワークＮＷのアクセスポイントＡＰの番号を発呼する。これにより、公衆網２のアクセスポイントＡＰまで固定的に接続され更にネットワークＮＷの交換機／ノード１に呼出が掛かるので、交換機／ノード１はこれに応答する。すると、アダプタ３では更に予め設定された暗号化パターンに従ってコード変換された利用者コードとその暗号化パターン番号とが交換機／ノード１に対して送出され、これとともに相手端末番号が送出される。

交換機／ノード１では、送られて来た暗号化パターン番号から暗号化パターンテーブルＹにより暗号化パターンを検索し、暗号化された利用者コードをその暗号化パターンによって復号（逆コード変換）した利用者コードと該暗号化パターン番号に対応して予め端末管理テーブルＸ（テーブルＹとでセキュリティテーブルを形成している）に記憶している利用者コードとを照合してそのアダプタ３の利用資格を確認した上で、相手端末番号を送出して自ネットワークＮＷの端末ＴＥ／ＴＥＬへの接続を行う。

このように暗号化されたセキュリティ情報を用いることより、よりセキュリティの高い通信／通話路を確保している。

〔発明が解決しようとする課題〕

このような従来のネットワークのセキュリティ・ガード方式では、網接続アダプタ内の利用者コード／暗号化パターン番号等のセキュリティ情報が網加入時にアダプタ側で設定されていたため、これが盗用される場合があり、また録音機等を組み合わせて盗用するケースも発生しているという問題点があった。

従って、本発明は、端末に接続された網制御装置の網接続アダプタから自営ネットワーク又は閉域ネットワークの交換機又はノードに公衆網上のアクセスポイントを介してアクセスする時に暗号

化されたセキュリティ情報を送出し該交換機又はノードで復号してセキュリティテーブルと照合するネットワークのセキュリティ・ガード方式において、暗号化されたセキュリティ情報が盗用される被害を最小限にすることを目的とする。

〔課題を解決するための手段及び作用〕

上記の課題を解決するため、本発明に係るネットワークのセキュリティ・ガード方式では、第1図に原理的に示すように、交換機又はノード1の側に設置された保守コンソール4から該交換機又はノード1に変更すべきセキュリティ情報①を入力し交換機又はノード1に記憶したセキュリティテーブルを変更するとともに該セキュリティテーブルに基づいて対応する該アダプタ3の暗号化されたセキュリティ情報を上記のセキュリティ情報①に設定・変更するようにしている。

従って、随時又は定期的にセキュリティ情報を遠隔設定・変更することができる。

一方、このようなコード変更を行う場合、第2図に示すように、公衆網2に対して例えば日官／閉域ネットワークA、Bが接続されているとすると、ネットワークBの利用者端末TEBの利用者コード及び暗号化パターンを変更しようとしたにもかかわらず、誤ダイヤルによりネットワークAの端末TEAの網接続アダプタに着信してしまい、その利用者コード等のセキュリティ情報を誤って変更してしまうことがある。

そこで、本発明では更に、各ネットワークNWに固有の識別子②を該網接続アダプタ3に予め設定しておき、該変更の前に該コンソール4から該交換機又はノード1を介して該アダプタ3に識別子②を送り、該アダプタ3において識別子②同士の照合を行い一致した時のみ該変更を行うことができる。

従って、異なるネットワーク間でセキュリティ情報を誤変更することがなくなる。

〔実　施　例〕

第3図は、本発明に係るネットワークのセキュリティ・ガード方式の一実施例を示したもので、交換機／ノードとしてのPBX1は、CPU11と、自システム内の各端末の利用者番号（端末に対応したアダプタの例えば電話番号）、利用者コード（暗号化されていない利用者コード）、暗号化パターン番号から成る端末管理テーブルX及び暗号化パターン番号から暗号化パターンを検索するための暗号化パターンテーブルY（テーブルXとでセキュリティテーブルを形成している）を記憶するメモリ12と、暗号変更情報送信用のPB（プッシュ・ボタン）信号発生部13と、通常着信識別信号(2100Hz)発生器14と、暗号変更通知信号(1800Hz)発生部15とで構成されており、網接続アダプタ3は、CPU31と、対応する端末の暗号化された利用者コード、その暗号化パターン番号並びにシステム識別子を記憶するメモリ32と、PB信号受信部33と、通常着信識別信号受信部34と、暗号変更通知信号受信部35とで構成されている。

このような実施例におけるセキュリティ情報の変更動作を第4図に示したシーケンスに沿って説明する。尚、設定動作も変更動作と同様にして行うことができるが、発生部14と受信部34は通常の送受信の場合のみに用いられ、設定・変更時には使用されない。

まず、保守コンソール4においてオペレータは設定・変更すべきセキュリティ情報を作成しておく。この場合、セキュリティ情報としては対応するアダプタ3の利用者番号と暗号化パターン番号が含まれていれば充分である。そして自動発信によりその利用者番号の端末に対応した網接続アダプタ3への発呼をPBX1及び公衆網2のアクセスポイントを介して行う。

これにより対応するアダプタ3が呼び出されて応答するので、PBX1は次に暗号変更通知を行うために発生部15から変更通知信号を発生し、これを受けてアダプタ3では受信部35で受信するとともに暗号変更の準備を行う。

一方、PBX1では、コンソール4で自動発信された暗号化パターン番号をCPU11が受けて

セキュリティテーブルを構成するテーブルYを検索することにより暗号化パターンを取り出し、この暗号化パターンに従ってやはりセキュリティテーブルを構成する端末管理テーブルXに記憶された利用者番号に対応する利用者コードを変換してアダプタ3に送る。そして、利用者番号に対応する古い暗号化パターン番号は新しく設定された暗号化パターン番号と置き換えられる。

この後、アダプタ3の側からは変更したセキュリティ情報が正しいか否かを確認するために、更新データをPBX1に返送し、PBX1において両者の照合を行うことが好ましい。

このようにしてセキュリティ情報の設定・変更が行われるが、第2図に示したように別のシステム間での誤変更が行われないようにするため各システムに固有の識別子が用いられる。

この識別子は第5図に示すように、Aネットワーク向けの装置及びBネットワーク向けの装置をそれぞれ工場Fの段階で製造するとき、併せて初期化装置20をも製造し、この初期化装置20にクBの網接続アダプタのセキュリティ情報を変更するような誤動作を未然に防ぐことができる。

尚、上記の説明ではセキュリティ情報の設定・変更のみについて扱ったが、通常の発呼シーケンスは第9図の場合と同じである。

〔発明の効果〕

このように、本発明のネットワークのセキュリティ・ガード方式によれば、交換機又はノードのコンソールから交換機又はノード及び網接続アダプタに変更すべきセキュリティ情報を送出して変更を行うように構成したので、一箇所のコンソールから全国の網接続アダプタに対して遠隔操作でセキュリティ情報の変更ができ、盗用された場合には即座に、また気付かない場合でも定期的にセキュリティ情報が変更できることとなり、盗用による被害を最小限に留めることができる。

また、ネットワーク毎に異なるシステム識別子をアダプタに予め設定しておき、変更の前に照合するようにすれば、異ネットワーク間での誤変更初期化装置20でしか設定できないシステム識別子を組み込んでおく。

そして、この初期化装置20を一緒に出荷すると、網接続アダプタ3の側においてネットワーク管理者が初期化装置20の識別子をアダプタ3に設定して加入者宅に設置する。

この後のセキュリティ情報の設定・変更動作を第6図に示したシーケンスにより説明する。

第4図のシーケンスと同様に暗号変更通知をPBX1からアダプタ3に行った後、PBX1に接続されたコンソール4からオペレータによってシステム識別子が入力され、このシステム識別子がPBX1のCPU11により対応するアダプタ3に送られると、アダプタ3の側では、送られて来たシステム識別子と上記のように設定されたシステム識別子とを比較照合し、一致した場合のみ応答信号をPBX1に送ることにより、PBX1は第4図の場合と同様にしてセキュリティ情報の設定・変更並びにその確認を行うことができる。

従って、ネットワークAのPBXがネットワークBの網接続アダプタのセキュリティ情報を変更するような誤動作を未然に防ぐことができる。

4. 図面の簡単な説明

第1図は本発明に係るネットワークのセキュリティ・ガード方式を原理的に示したブロック図、

第2図は本発明に係るネットワークのセキュリティ・ガード方式において異ネットワーク間の誤変更が生ずる場合を説明した図、

第3図は本発明方式の一実施例を示したブロック図、

第4図は本発明方式によるセキュリティ情報の変更動作を説明するためのシーケンス図、

第5図は本発明においてシステム識別子の設定を説明するための図、

第6図はシステム識別子を用いてセキュリティ情報の変更をする場合のシーケンス図、

第7図は公衆網に接続された自営／閉域ネットワークの構築図、

第8図及び第9図は本発明及び従来例に共通の発呼シーケンスを説明するための図、である。

第1図において、

1…交換機／ネットワークノード、

2…公衆網、

3…網接続アダプタ、

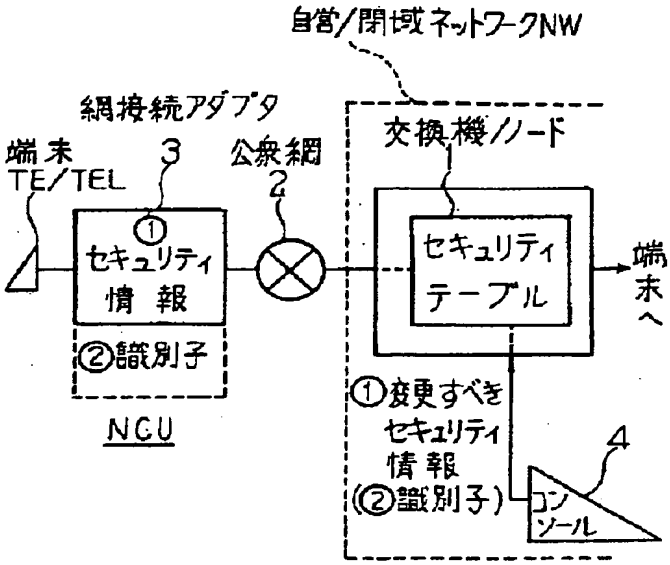
4…保守コンソール、

TE、TEL…端末、

NW…自営／閉域ネットワーク。

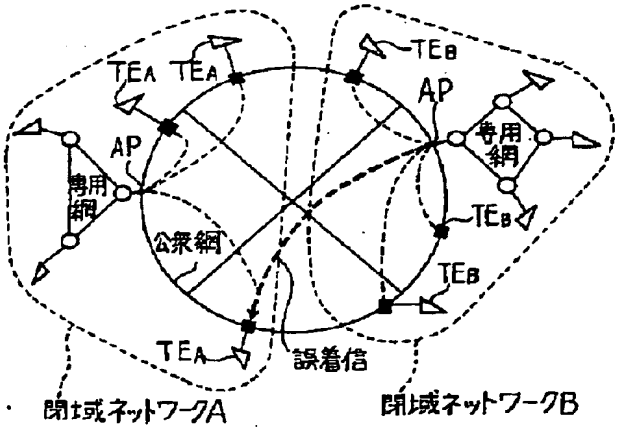
図中、同一符号は同一又は相当部分を示す。

代理人　弁理士　茂泉　修司



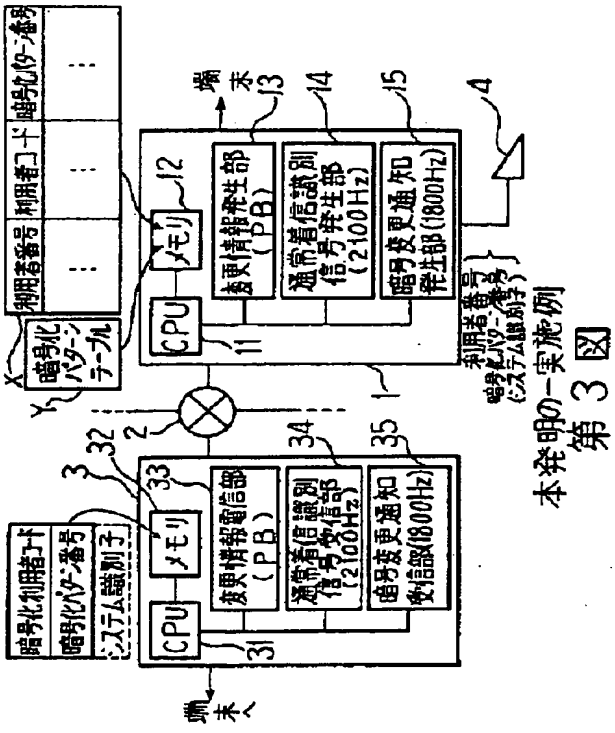
本発明の原理図

第1図



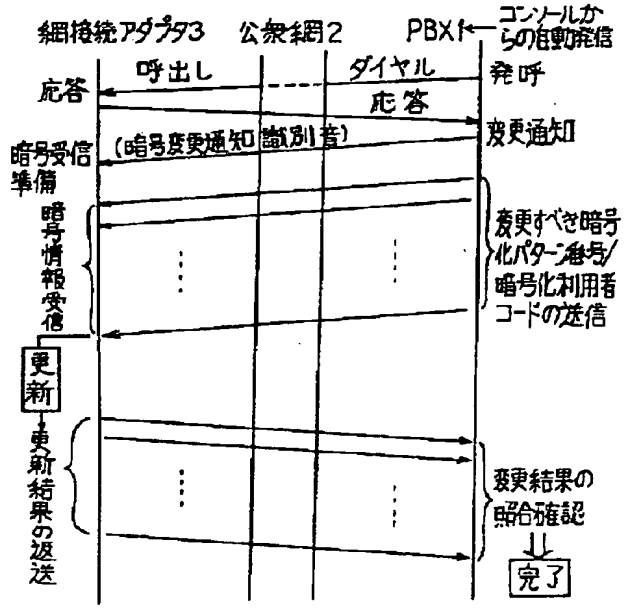
誤変更の説明図

第2図



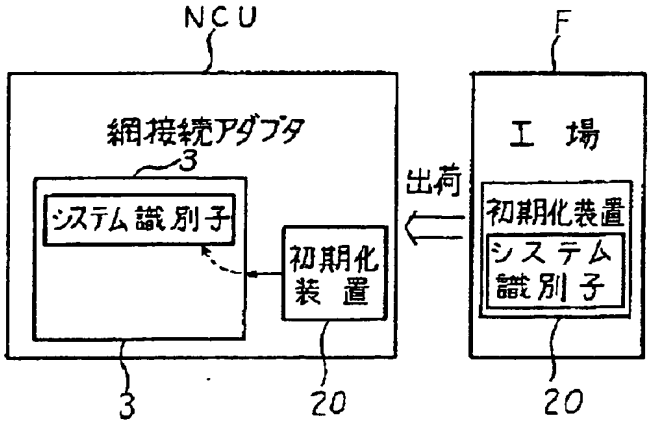
本発明の一実施例

第3図



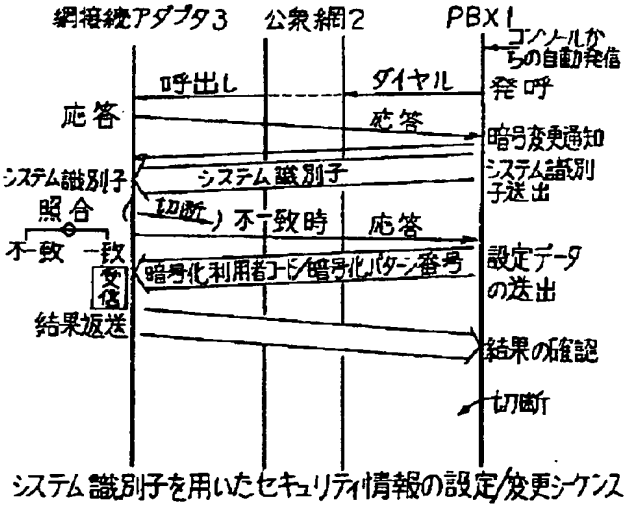
セキュリティ情報の変更時のシーケンス

第 4 図



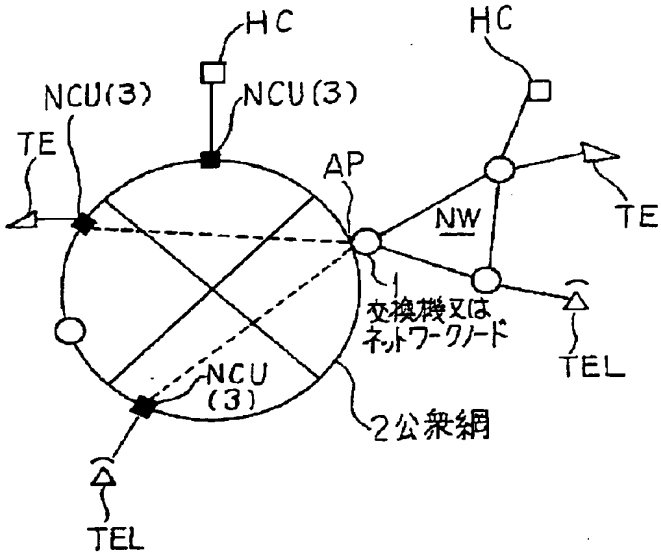
システム識別子の設定

第 5 図



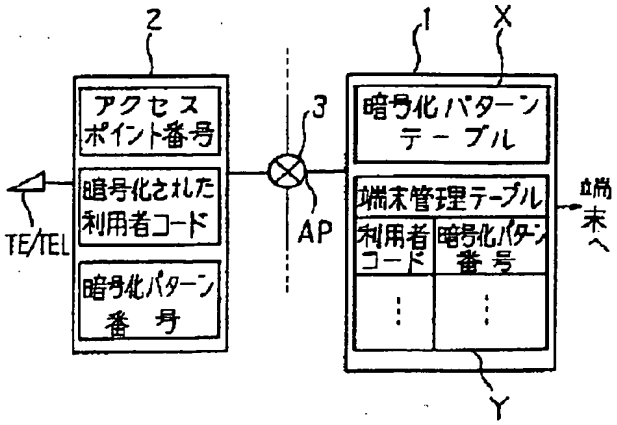
システム識別子を用いたセキュリティ情報の設定/変更シーケンス

第 6 図



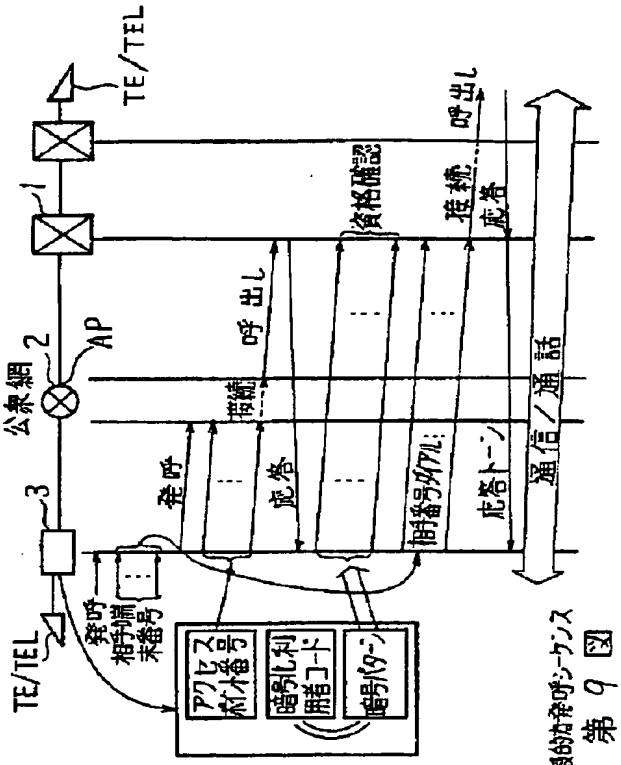
自営/閉域ネットワーク構築図

第 7 図



接続動作の概念図

第 8 図



第 9 図